IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: Date: August 21, 2003

Applicant(s):	Philip D. MacKenzie
Case:	15
Serial No.:	10/600,687
Filing Date:	June 20, 2003
Group:	To Be Assigned
Examiner:	To Be Assigned

Title: Methods and Apparatus for Providing Secure Two-Party Public Key Cryptosystems

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to 37 C.F.R. §§1.56, 1.97 and 1.98, Applicant's attorney wishes to bring to the attention of the Patent and Trademark Office the following documents listed on the accompanying Form PTO-1449. A copy of each listed document is enclosed.

1. V. Shoup et al., "Securing Threshold Cryptosystems against Chosen Ciphertext Attack," EUROCRYPT '98, pp. 1-22, 1998.

2. R. Canetti et al., "An Efficient *Threshold* Public Key Cryptosystem Secure Against Adaptive Chosen Ciphertext Attack," EUROCRYPT '99 (LNCS 1592), pp. 90-105, 1999.

3. M. Abe, "Robust Distributed Multiplication without Interaction," CRYPTO '99 (LNCS 1666), pp. 130-147, 1999.

4. S. Jarecki et al., "Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures," EUROCRYPT 2000 (LNCS 1807), pp. 221-242, 2000.

5. P-A. Fouque et al., "Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks," ASIACRYPT '01 (LNCS 2248), pp. 351-368, 2001.

6. M. Bellare et al., "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," 1st ACM Conference on Computer and Communications Security, pp. 62-73, November 1993.

7. R. Canetti et al., "The Random Oracle Methodology, Revisited," 30th ACM Symposium on Theory of Computing, pp. 209-218, 1998.

8. R. Cramer et al., "A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack," CRYPTO '98 (LNCS 1462), pp. 13-25, 1998.

9. R. Cramer et al., "Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption," EUROCRYPT 2001 (LNCS 2332), pp. 45-64, 2002.

10. S. Micali, "Fair Public-key Cryptosystems," CRYPTO '92 (LNCS 740), pp. 113-138, 1992.

11. N. Asokan et al., "Optimistic Protocols for Fair Exchange," 3rd ACM Conference on Computer and Communications Security, pp. 1-23, 1996.

12. P. MacKenzie et al., "Networked Cryptographic Devices Resilient to Capture," DIMACS Technical Report 2001-19, pp. 1-38, May 2001.

13. P. MacKenzie et al., "Two-Party Generation of DSA Signatures," CRYPTO 2001 (LNCS 2139), pp. 137-154, 2001.

14. R. Cramer et al., "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols," CRYPTO '94 (LNCS 839), pp. 174-187, 1994.

15. U. Feige et al., "Witness Indistinguishable and Witness Hiding Protocols," 22nd ACM Symposium on Theory of Computing, pp. 416-426, 1990.

16. T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Volume 31, pp. 469-472, 1985.

17. J. Camenisch et al., "Proof Systems for General Statements about Discrete Logarithms," Technical Report TR 260, Department of Computer Science, ETH Zurich, pp. 1-13, March 1997.

18. I. Damgård, "Efficient Concurrent Zero-Knowledge in the Auxiliary String Model," EUROCRYPT 2000 (LNCS 1807), pp. 418-430, 2000.

19. A. Fiat et al., "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," CRYPTO '86 (LNCS 263), pp. 186-194, 1987.

It is believed that there is no fee due in conjunction with the filing of this Information Disclosure Statement. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Ryan, Mason & Lewis, LLP Deposit Account No. 50-0762** as required to correct the error.

The filing of this Information Disclosure Statement shall not be construed as a representation that a search has been made, or as an admission that the information cited is considered to be material to patentability, or as a representation that no other material information exists.

Respectfully submitted,

William E. Lewis

Date: August 21, 2003

William E. Lewis
Reg. No. 39,274
Attorney for Applicant(s)
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946

FORM PTO-1449 (MODIFIED)

LIST OF PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT

Applicant(s):	Philip D. MacKenzie
Case:	15
Serial No.:	10/600,687
Filing Date:	June 20, 2003
Group:	To Be Assigned

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NO.	DATE	NAME	CLASS/SUBCLASS	FILING DATE IF APPROPRIATE
___					

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NO.	DATE	COUNTRY	CLASS/SUBCLASS	TRANSLATION YES	TRANSLATION NO

OTHER DOCUMENTS

EXAMINER INITIAL	REF NO.	AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.
___	1.	V. Shoup et al., “Securing Threshold Cryptosystems against Chosen Ciphertext Attack,” EUROCRYPT ‘98, pp. 1-22, 1998.
___	2.	R. Canetti et al., “An Efficient *Threshold* Public Key Cryptosystem Secure against Adaptive Chosen Ciphertext Attack,” EUROCRYPT ‘99 (LNCS 1592), pp. 90-105, 1999.
___	3.	M. Abe, “Robust Distributed Multiplication without Interaction,” CRYPTO ‘99 (LNCS 1666), pp. 130-147, 1999.
___	4.	S. Jarecki et al., “Adaptively Secure Threshold Cryptography: Introducing Concurrency, Removing Erasures,” EUROCRYPT 2000 (LNCS 1807), pp. 221-242, 2000.
___	5.	P-A. Fouque et al., “Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks,” ASIACRYPT ‘01 (LNCS 2248), pp. 351-368, 2001.
___	6.	M. Bellare et al., “Random Oracles are Practical: A Paradigm for Designing Efficient Protocols,” 1st ACM Conference on Computer and Communications Security, pp. 62-73, November 1993.
___	7.	R. Canetti et al., “The Random Oracle Methodology, Revisited,” 30th ACM Symposium on Theory of Computing, pp. 209-218, 1998.
___	8.	R. Cramer et al., “A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack,” CRYPTO ‘98 (LNCS 1462), pp. 13-25, 1998.

Examiner ______________________ Date Considered ______________________

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

FORM PTO-1449 (MODIFIED)

LIST OF PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT

Applicant(s):	Philip D. MacKenzie
Case:	15
Serial No.:	10/600,687
Filing Date:	June 20, 2003
Group:	To Be Assigned

OTHER DOCUMENTS (cont'd.)

EXAMINER INITIAL	REF NO.	AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.
___	9.	R. Cramer et al., "Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption," EUROCRYPT 2001 (LNCS 2332), pp. 45-64, 2002.
___	10.	S. Micali, "Fair Public-key Cryptosystems," CRYPTO '92 (LNCS 740), pp. 113-138, 1992.
___	11.	N. Asokan et al., "Optimistic Protocols for Fair Exchange," 3rd ACM Conference on Computer and Communications Security, pp. 1-23, 1996.
___	12.	P. MacKenzie et al., "Networked Cryptographic Devices Resilient to Capture," DIMACS Technical Report 2001-19, pp. 1-38, May 2001.
___	13.	P. MacKenzie et al., "Two-Party Generation of DSA Signatures," CRYPTO 2001 (LNCS 2139), pp. 137-154, 2001.
___	14.	R. Cramer et al., "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols," CRYPTO '94 (LNCS 839), pp. 174-187, 1994.
___	15.	U. Feige et al., "Witness Indistinguishable and Witness Hiding Protocols," 22nd ACM Symposium on Theory of Computing, pp. 416-426, 1990.
___	16.	T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, Volume 31, pp. 469-472, 1985.
___	17.	J. Camenisch et al., "Proof Systems for General Statements about Discrete Logarithms," Technical Report TR 260, Department of Computer Science, ETH Zurich, pp. 1-13, March 1997.
___	18.	I. Damgård, "Efficient Concurrent Zero-Knowledge in the Auxiliary String Model," EUROCRYPT 2000 (LNCS 1807), pp. 418-430, 2000.
___	19.	A. Fiat et al., "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," CRYPTO '86 (LNCS 263), pp. 186-194, 1987.

Examiner ______________________ Date Considered ______________________

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.